Amendments to the Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1-9. (Canceled)

10. (Currently Amended) A method for providing access management, comprising:

(a) authenticating a user to a first and a second server machine, whereby the first and the second server machine are configured to comprise a secured item; and

(b) preventing access to a first one of the first and the second server machines ~~machine~~ while the user is accessing a second one of the first and the second server machines ~~machine~~;

wherein the user is disconnected from the first one of the first and the second server machines ~~machine~~ before being connected to the second one of the first and the second server machines ~~machine~~.

11. (Previously Presented) The method as recited in claim 29, wherein step (a1) authenticates both the user and a client machine being used by the user.

12. (Previously Presented) The method as recited in claim 10, wherein the first and the second server machine are access points for the user to gain access to the secured item.

13. (Previously Presented) The method as recited in claim 29, wherein:

when the user is at a first location, the user interacts over a network with the first server machine, and

when the user is at a second location, the user interacts over a network with the second server machine using a second client machine at the second location.

14. (Previously Presented) The method as recited in claim 30, wherein the method further comprises:

determining, prior to steps (b1), (b2), (b3), and (b4), whether the user is permitted to gain access from a second location to the secured item via the second server machine.

15. (Previously Presented) The method as recited in claim 29, wherein step (a1) occurs while the user is at a first location, and wherein step (a2) occurs while the user is at a second location.

16. (Previously Presented) The method as recited in claim 17, wherein the method further comprises:

(a4) upon receiving the current access request to access the secured item via the second server machine, determining permitted locations from which the user is permitted to access-the secured item;

(a5) determining whether the second location is one of the permitted locations for the user; and

(a6) bypassing steps (b1), (b2), (b3), and (b4) when step (a5) determines that the second location is not one of the permitted locations for the user.

17. (Previously Presented) The method as recited in claim 30, wherein:

when the user is at a first location, the user interacts over a network with the first server machine using a first client machine at the first location, and

when the user is at a second location, the user interacts over a network with the second server machine using a second client machine at the second location.

18. (Currently Amended) A computer readable medium containing instructions for controlling at least one processor by a method comprising:

(a) authenticating a user to a first and a second server machine, whereby the first and the second server machine are configured to comprise a secured item; and

(b) preventing access to a first one of the first and the second server machines ~~machine~~ while the user is accessing a second one of the first and the second server machines ~~machine~~;

wherein the user is disconnected from the first one of the first and the second server machines ~~machine~~ before being connected to the second one of the first and the second server machines ~~machine~~.

19. (Previously Presented) The computer readable medium as recited in claim 31, wherein:

when the user is at a first location, the user interacts over a network with the first server machine, and

when the user is at a second location, the user interacts over a network with the second server machine using a second client machine at the second location.

20. (Previously Presented) The computer readable medium as recited in claim 32, further comprising:

determining, prior to the reconfiguring of either the first local module at the first server machine or the second local module at the second server machine, whether the user is permitted to gain access from a second location to the secured item via the second server machine.

21. (Currently Amended) A system for providing access management, comprising:

an access control device, wherein the access control device authenticates a user to a first and a second server machine, whereby the first and the second server machine are configured to comprise a secured item, and prevents access to a first one of the first and the second server machines ~~machine~~ while the user is accessing a second one of the first and the second machines ~~machine~~;

wherein the user is disconnected from the first one of the first and the second server machines ~~machine~~ before being connected to the second one of the first and the second server machines ~~machine~~.

22. (Previously Presented) The computer readable medium as recited in claim 31, wherein step (a1) authenticates both the user and a client machine being used by the user.

23. (Previously Presented) The computer readable medium as recited in claim 32, further comprising:

determining, prior to reconfiguring the first local module at the first server machine and the second local module at the second server machine, whether the user is permitted to gain access from a second location to the secured item via the second server machine.

24. (Previously Presented) The computer readable medium as recited in claim 33, wherein step (a) further comprises:

(a4) upon receiving the current access request to access the secured item via the second server machine, determining permitted locations from which the user is permitted to gain access to the secured item;

(a5) determining whether the second location is one of the permitted locations for the user; and

(a6) bypassing steps (b1), (b2), (b3), and (b4) when step (a5) determines that the second location is not one of the permitted locations for the user.

25. (Previously Presented) The system as recited in claim 21, wherein the access control device authenticates both the user and a client machine being used by the user.

26. (Previously Presented) The system ~~of~~ as recited in claim 21, wherein the first and the second server machine are access points for the user to gain access to the secured item.

27. (Previously Presented) The system as recited in claim 35, wherein the access control device determines, prior to reconfiguring the first local module at the first server machine and the second local module at the second server-machine, whether the user is permitted to gain access from a second location to the secured item via the second server machine.

28. (Canceled)

29. (Previously Presented) The method as recited in claim 10, wherein step (a) comprises:

(a1) authenticating the user with the first server machine with respect to a previous access request;

(a2) subsequently receiving a current access request via the second server machine; and

(a3) authenticating the user with the second server machine with respect to the current access request.

30. (Previously Presented) The method as recited in claim 29, wherein step (b) comprises:

(b1) upon receiving the current access request via the second server machine, identifying a first local module previously supporting the user at the first server machine;

(b2) reconfiguring the first local module at the first server machine to remove support for the user at the first server machine;

(b3) identifying a second local module to support the user at the second server machine; and

(b4) reconfiguring the second local module at the second server machine to add support for the user at the second server machine.

31. (Previously Presented) The computer readable medium as recited in claim 18, wherein step (a) comprises:

(a1) authenticating the user with the first server machine with respect to a previous access request;

(a2) subsequently receiving a current access request via the second server machine; and

(a3) authenticating the user with the second server machine with respect to the current access request.

32. (Previously Presented) The computer readable medium as recited in claim 31, wherein step (b) comprises:

(b1) upon receiving the current access request via the second server machine, identifying a first local module previously supporting the user at the first server machine;

(b2) reconfiguring the first local module at the first server machine to remove support for the user at the first server machine;

(b3) identifying a second local module to support the user at the second server machine; and

(b4) reconfiguring the second local module at the second server machine to add support for the user at the second server machine.

33. (Previously Presented) The computer readable medium as recited in claim 32, wherein:

when the user is at a first location, the user interacts over a network with the first server machine using a first client machine at the first location, and

when the user is at a second location, the user interacts over a network with the second server machine using a second client machine at the second location.

34. (Previously Presented) The system as recited in claim 21, wherein the access control device:

authenticates the user with the first server machine with respect to a pervious access request;

subsequently receives a current access request via the second server machine; and

authenticates the user with the second server machine with respect to the current access request.

35. (Previously Presented) The system as recited in claim 34, wherein the access control device:

identifies a first local module previously supporting the user at the first server machine upon receiving a current access request to access the secure item via the second server machine;

reconfigures the first local module at the first server machine to remove support for the user at the first server machine;

identifies a second local module to support the user at the second server machine; and

reconfigures the second local module at the second server machine to add support for the user at the second server machine.